Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 61 (2015) 233 – 239

Procedia Computer Science

Complex Adaptive Systems, Publication 5
Cihan H. Dagli, Editor in Chief
Conference Organized by Missouri University of Science and Technology
2015-San Jose, CA

Mitigating Counterfeit Part Intrusions with Enterprise Simulation

Douglas A. Bodner*

Tennebaum Institute, Georgia Institute of Technology, Atlanta, Georgia 30308 USA

Abstract

In recent years, counterfeit parts have infiltrated the defense supply chain, which provides replacement parts and sub-systems for deployed systems. This creates a significant amount of risk. Both government and industry have formulated and implemented various policy initiatives to address the problem, including inspections, penalties and trusted sourcing. However, the problem is still on-going. Additional policies are under consideration, and the unintended effects of policies are not known. To study the problem and potential policy solutions, we present an enterprise simulation model of counterfeit parts intrusion and policy alternatives. The model reflects the defense enterprise, tiers of suppliers, counterfeiters and other government policy actors. Interactions of these actors and their reactions to events and policies form an important part of the enterprise system behavior. Policies, their effects and their interactions are detailed in this multi-stakeholder environment.

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology

Keywords: Enterprise systems; enterprise simulation; socio-technical modeling; counterfeit parts; policy simulator

1. Introduction

In recent years, counterfeit parts have infiltrated the defense supply chain, which provides replacement parts and sub-systems for deployed systems[1,2,3]. This situation creates a significant amount of risk, since counterfeit constituent parts may degrade performance of systems and may also cause safety concerns. For instance, many counterfeit parts are used or defective parts passed as new[4]. Thus, they typically would have worse reliability than would a genuine new part. Others are fake parts imprinted with a logo representing the intellectual property (IP) rights holder.

* Corresponding author. Tel.: +1-404-894-2363.
E-mail address: doug.bodner@gatech.edu

Peer-review under responsibility of scientific committee of Missouri University of Science and Technology
doi:10.1016/j.procs.2015.09.203

Primarily, counterfeit parts have been electronics, such as integrated circuits (ICs), imported into the United States[5]. When counterfeits occur as system components, such as ICs, they are generally difficult to detect once assembled into a higher-order sub-system. Thus, it is important to detect such counterfeits prior to assembly into higher-order sub-systems. For any one end-product system, though, the defense supply chain can be quite complex. For example, the supply chain for the F-35 Joint Strike Fighter has approximately 1,580 suppliers arranged in multiple tiers[6]. Other programs have similarly complex supply chains. A supplier providing a component such as an IC may have that IC pass through a series of assembly operations whereby the sub-system into which it is assembled is itself assembled into a higher order sub-system, which in turn is assembled into another higher-order sub-system. The lead systems integrator (LSI) has overall responsibility for the end-product system, but may not even have visibility into the supply chain tiers that extend past its direct suppliers. This presents a vulnerability to counterfeiting, since intrusion may occur many times removed from the LSI or depots that sustain systems.

Counterfeiting is driven by a variety of factors. As electronics become commoditized, the original component manufacturers (OCMs) leave the market, forcing suppliers using those products to find alternative sources. This increases the probability of counterfeiting due to less reliable sourcing. This is compounded by the increasing lifespans of deployed systems, requiring replacement parts for many years after an OCM has potentially left the market. In electronics, most manufacturing has been off-shored, where IP protections typically are less stringent than in the U.S. Counterfeiters clearly have found profit opportunities, as used components can be passed as new for profit. Additional drivers come into play, as well[7].

This paper presents enterprise modeling as a way to test different policies for addressing the problem of counterfeit parts. To wit, Section 2 describes the nature of the counterfeit parts problem as an enterprise problem. Enterprise problems and models to address them are a relatively new area of research. Next, Section 3 presents an enterprise simulation model of the counterfeit parts problem. Section 4 discusses policies, their interactions and results to date. Finally, Section 5 concludes and provides avenues of future research.

2. Counterfeit Parts Infiltration as an Enterprise Problem

The issue of counterfeit parts in the defense supply chain cuts across many different organizations and organization types. For purposes of modeling, we consider this set of organizations as an enterprise in the sense that they are directing their efforts and resources toward common goals[8]. In this case, the goal is to prevent counterfeit infiltrations for purposes of national security, as well as health and safety. This is a public-private enterprise encompassing government agencies and private firms (e.g., defense suppliers)[9]. No single organization has full control of the entire enterprise. The Department of Defense (DoD) issues guidelines and policies to address issues such as counterfeiting. However, these policies typically leave some discretion to individual defense programs and suppliers. Moreover, suppliers can choose whether or not to participate in the defense supply chain. In addition to DoD, other agencies such as Customs and Border Protection (CBP) and the Department of Justice (DoJ) have jurisdiction over aspects of counterfeiting such as inspection and interdiction at import locations and prosecution of offenders, respectively.

Of course, the counterfeiters operate as part of the enterprise, being that they are suppliers, but they operate largely outside enterprise control. They adapt methods and strategies to government actions. For instance, a counterfeiter may improve the quality of a counterfeit item to avoid detection via improved testing. Likewise, a counterfeiter may adjust its supply channels to avoid interdiction at points with improved detection. Similarly, government agencies and private firms adapt to new counterfeiting threats with policies and actions. Thus, this enterprise as with many operates as a complex adaptive system[10], which is characterized by multiple independent agents that react to information and incentives in ways that create unpredictable overall system behavior.

Enterprise modeling and simulation is a relatively new approach to studying complex systems with organizational elements[11,12,13]. Enterprise modeling often is used to identify policies to solve problems, as well as characterize secondary or unintended effects of policies[14,15]. In the counterfeit parts domain, the DoD has a number of different policy levers that it can apply[16,17,18,19,20]. For instance, it can mandate that programs use qualified suppliers for all components and sub-systems that comprise a deployed system, where a qualified supplier is defined by a specific qualification process. It can impose penalties on suppliers who pass counterfeit components in their sub-systems. It can mandate testing of components at entry points to DoD programs. Each policy has strengths and potential

drawbacks. For instance, testing is expensive and can yield significant false positives[20]. Individual programs may enact policies, as well. In addition, other government agencies such as CBP and DoJ have policy influence on counterfeiting. The intent here is to use enterprise modeling to test such policies for effectiveness before implementation in the real enterprise.

3. Enterprise Simulation Model of Counterfeit Parts Infiltration

The enterprise simulation model for counterfeit parts is based on an enterprise modeling methodology[21,22] and a generic supply chain based enterprise framework[7]. The framework is divided into five interacting models summarized below.

- A *systems and constituents model* represents the various systems, sub-systems and components plus the architecture that relates them to one another. This is captured in a bill-of-materials.
- A *supply chain model* represents the factories and inventories for each component and sub-system, plus the flow of those constituents to the LSI for final assembly into a system and to depots and other locations for use in sustainment.
- An *enterprise actor model* represents the various suppliers that own factories and other locations in the supply chain model and their behavior over time as they react to changing conditions and policies.
- A *policy actor model* represents the various agencies and other organizations that enact policies affecting counterfeit parts.
- An *exogenous environment model* represents the external world and its effect on counterfeiting and anti-counterfeiting policies.

The model is implemented using AnyLogic™ 7, primarily as an agent-based simulation with Java™ class extensions. The focus here is on the first four models above.

Specifically, the system and constituents model contains two end-product systems – a fighter jet and a high-altitude unmanned aerial vehicle (UAV). The bill of materials contains two levels of sub-system objects for each, as well as one level of component objects. The components correspond to electronics that may be counterfeited. Note that only the sub-systems and components subject to counterfeit risk are included, as inclusion of all sub-systems and components would be computationally expensive. In the model, systems, sub-systems and components are instantiated as agents that reference information in the bill of materials and execute behaviors.

Correspondingly, a supply chain provides the various sub-systems and components. Factory agents fabricate components and ship them to other factories for assembly into sub-systems. These sub-systems are then shipped to other factory agents where they are assembled into higher-order sub-systems. These sub-systems are mostly line-replaceable units (LRUs) that feed directly into the end-product system, and that can be repaired and replaced into in-service systems. For sustainment, spare sub-systems and components are shipped to depot agents where maintenance, repair and replacement are performed. In-service systems have needs for these operations, in turn creating demand for sub-systems and components. Some component suppliers are foreign, in which case the components are sent through customs agents where they may be inspected. Similarly, suppliers may institute control points where components are tested prior to transfer from the consumer supply chain to a DoD program. The systems and constituents model and the supply chain model are shown in Figure 1.

Factories are owned by supplier agents in the enterprise actor model. The supply chain evolves over time due to the actions of these suppliers. An OCM supplier may decide to leave the market for a particular component when it loses profitability, for example. This marks the beginning of a component's journey to obsolescence. This supplier sends a notification to all suppliers that make sub-systems using this component and then shuts down production. Those suppliers then search for an alternate source. Potentially available options include franchise manufacturers (authorized by the OCM that holds IP rights), authorized distributors (likewise authorized by the OCM), brokers (non-authorized distributors), or from potentially unknown sources (e.g., internet sites). In some cases, certain obsolete components are available from a government-certified firm. Aside from the government-certified firms, this represents a series of sources with increasing risk of counterfeit infiltration.

A percentage of foreign suppliers provide counterfeit components. Typically, the counterfeit components are imported via a broker. A percentage of brokers knowingly import counterfeit components. A percentage of imported components are inspected at a customs point. Those identified as counterfeits are called "counterfeit suspects." CBP may enlist the aid of the IP holder to help with suspect identification. Suspects are interdicted. It should be noted that suspects can be either true positives (counterfeits) or false positives (genuine components misidentified as counterfeits). Similarly, components are tested at DoD control points (using more sophisticated methods). Such tests may be destructive, and they also involve the possibility of false positives. A false positive results in discarded good product.

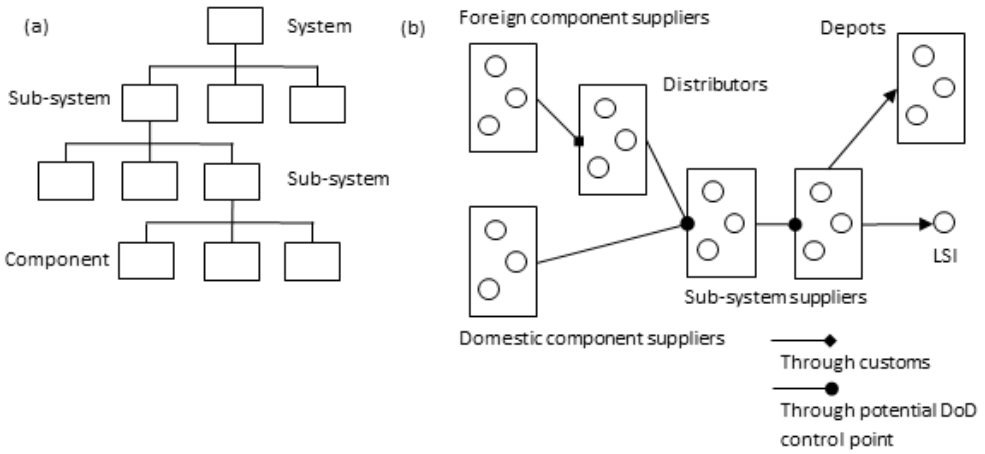

Fig. 1. (a) system and constituent model; (b) supply chain model.

Identification of counterfeit suspects can result in referral of the importer to DoJ for prosecution. Since the control points are operated by suppliers, it should be noted that there is substantial lack of knowledge in the defense industrial base about proper reporting of counterfeit suspects[9]. The DoJ may indict knowing importers as in a recent incident[23], in which case they are shut down, and others seeing the consequences may decide to exit the business. The DoJ indicts based on its level of resources and on the priority between IP violations and fraud. IP violations occur when an IP holder's logo is forged onto a fake component. Fraud, on the other hand, involves passing used or defective components as new.

4. Policy Modeling, Effects and Interactions

The policy model contains the following agents that can adopt anti-counterfeiting policies.

- The DoD can set policies regarding sourcing of parts over all programs. One policy currently being adopted is that such parts must be purchased from qualified suppliers. It is assumed here that qualified suppliers include OCMs, franchisees and authorized distributors. Any parts purchased from other sources must be tested at a control point. This policy would apply to all sub-systems at or above a certain level of criticality (from one to five, with five being the highest).
- DoD programs select a strategy to manage obsolete sub-systems. One such strategy is to perform a design refresh, while another is to purchase a "lifetime buy" of components from an OCM before it exits the market.
- DoJ can set the resource level that it expends on counterfeiting cases, and it can also prioritize IP cases versus fraud cases.
- CBP can set the percentage of component lots that it inspects, and it can also set whether it cooperates with IP holders to identify suspects.

It should be noted that there certainly are other policies that can be added, for example tracking components throughout their lifecycle, enforcing penalties on suppliers that (unknowingly) pass counterfeit components in their sub-systems, or having programs be able to set a level of testing or supplier qualification themselves.

In addition, an analyst can set the percentage of foreign component suppliers that counterfeit and the risk behaviors of counterfeiters as two factors in the exogenous environment model. The simulation is implemented so that the policy options and exogenous environment options are selectable on an interface display, which also shows the consequences of these selections in terms of effectiveness (counterfeit suspects identified and counterfeit escapes), as well as cost. The interface is shown in Figure 2.

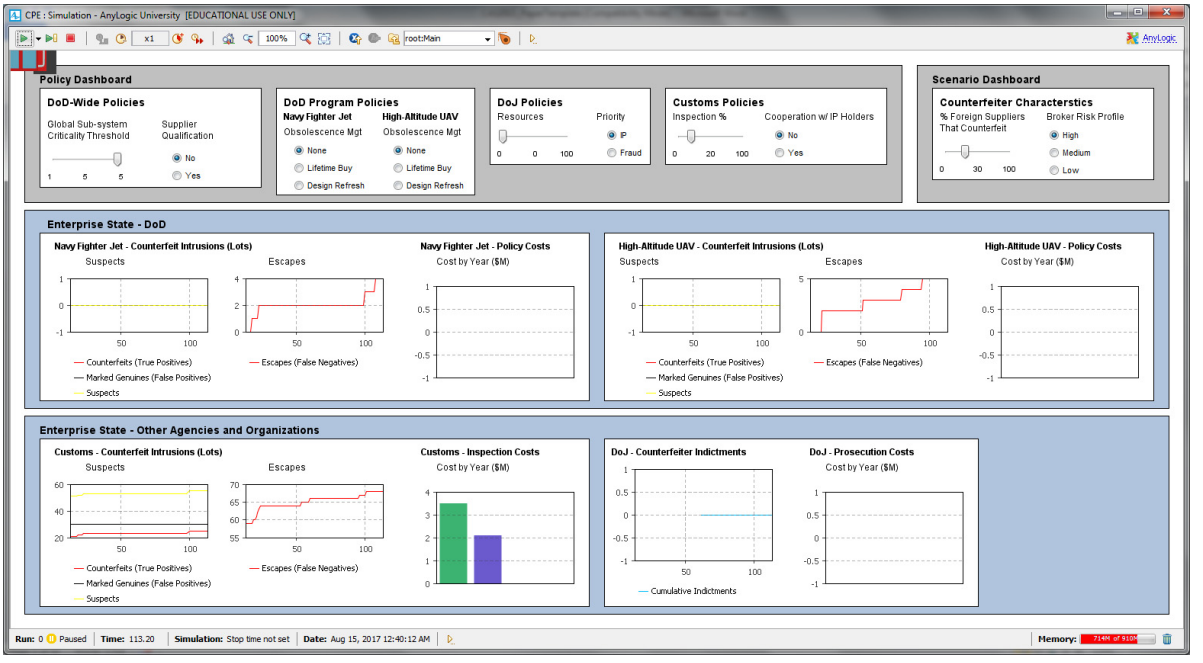

Fig. 2. Simulation interface.

In the simulation run reflected in the figure, the DoD and DoD program policy options are not enabled. Hence, there are no policy costs incurred. The number of escapes (counterfeit component lots passing into the program) are shown over time for each program. Since qualification/testing is not enabled, there are no suspects reported at the program level. Customs inspects 20% of incoming lost randomly, and the number of suspects and escapes are shown over time. It should be noted that many of the escapes from Customs are still in the supply chain and have not made it yet to a program. Finally, DoJ has not issued any indictments during the simulated time period.

Currently, the model is populated with test data. The goal is to provide data that is realistic for a given scneario using a reasonably generic data structure. The motivation here is that real data is difficult to verify for many aspects of the model due to the sensitive nature of the problem, distributed nature of data across multiple agencies, and lack of knowledge about counterfeiters and their operations. Thus, an analyst would be responsible for populating the model with data from their scenario of interest.

To illustrate use of the model, the following scenarios are analyzed. Table 1 shows average results for the various metrics over the four different scenarios for a ten year period with ten replications.

- Scenario 1. Baseline scenario from Figure 2.
- Scenario 2. Baseline scenario plus supplier qualification for all sub-systems.

- Scenario 3. Baseline scenario plus increased resources for prosecution (50%).
- Scenario 4. Scenarios 2 and 3 combined.

Table 1. Example counterfeiting scenarios.

Model outputs (averaged over ten replications)	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Escapes – fighter jet program (lots)	56.3	13.8	53.8	12.1
Suspects – fighter jet program (lots)	0	72.3	0	70.3
Policy cost – fighter jet program ($M)	0	30.4	0	30.7
Escapes – UAV program (lots)	51.7	11.6	48.9	11.4
Suspects – UAV program (lots)	0	69.7	0	65.2
Policy cost – UAV program ($M)	0	31.9	0	32.5
Escapes – Customs (lots)	640.2	636.0	635.2	632.1
Suspects – Customs (lots)	595.3	608.7	598.8	580.5
Policy cost – Customs ($M)	56.1	55.7	57.9	57.1
Indictments – DoJ (lots)	0	0	65.4	66.5
Policy cost – DoJ ($M)	0	0	53.6	52.1

In this relatively simple example, supplier qualification reduces counterfeit rates (escapes) at the programs. Likewise, increasing DoJ resources appears to have an impact on counterfeit rates in general (escapes and suspects), although not very large. Combining these two approaches yields a decrease in counterfeits, but also at a policy cost of $172.4M versus that of $56.1M for the baseline scenario. It should be noted that there is a one-time cost associated with policy start-up (e.g., qualification proccess for suppliers), as well as a recurring cost. The example demonstrates the goal to provide an environment where trade-offs between counterfeits, costs and other metrics can be evaluated.

5. Conclusions and Future Research

Counterfeit parts continue to be a potentially serious problem in the defense supply chain. This paper has presented an enterprise model addressing the problem of counterfeit parts in the defense supply chain. The goal is to use this model as an aid to test anti-counterfeiting policies before implementation and to gain insight into potential interactions among policies. Such a model can be used in a setting with different stakeholder types so that different perspectives can be shared on how potential solutions affect different parts of the enterprise.

In developing the model, a number of stakeholders from the defense and related communities were engaged in discussion sessions[7]. These sessions will continue to be used to refine the model, add policies, and test different scenarios and policies. The current model illustrates cost consequences. Current work is aimed at providing a system reliability consequence for counterfeit components, since counterfeits can have an impact on reliability and hence availability. In addition, current work is ongoing to use the model as an input to other systems-of-systems design tools seeking for purposes of system selection.

Acknowledgements

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract HQ0034-13-D-0004. SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the United States Department of Defense.

References

1. Government Accountability Office. DoD should leverage ongoing initiatives in developing its program to mitigate risk of counterfeit parts. Report GAO-10-389. Washington, DC: Author; 2010.
2. Government Accountability Office. Suspect counterfeit electronic parts can be found on internet purchasing platforms. Report GAO-12-375. Washington, DC: Author; 2012.
3. Stradley J, Karraker D. The electronic part supply chain and risks of counterfeit parts in defense applications. *IEEE Trans Compon Packag Technol* 2006;**29**:703-5.
4. Guin U, Dimase D, Tehranipoor M. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. *J Electron Test* 2014.
5. Pecht M, Tiku S. Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. *IEEE Spectrum* 2006;**43**:37-46.
6. Government Accountability Office. F-35 Joint Strike Fighter: problems completing software testing may hinder delivery of expected warfighting capabilities. Report GAO-14-322. Washington, DC: Author, 2014.
7. Bodner DA. Enterprise modeling framework for counterfeit parts in defense systems. *Proc Comput Sci* 2014;**36**:425-31.
8. Rouse WB. Enterprises as systems: essential challenges and approaches to transformation. *Syst Engineer* 2005;**82**:138-50.
9. Department of Commerce. Defense industrial base assessment: counterfeit electronics. Washington, DC: Author, 2012.
10. Miller JH, Page SE. *Complex adaptive systems: an introduction to computational models of social life*. Princeton, NJ: Princeton University Press; 2007.
11. Barjis J. Enterprise modeling and simulation within enterprise engineering. *J Enterprise Transform* 2011;**1**:185-207.
12. Bodner DA, Lee IH. Organizational simulation in support of global manufacturing enterprises. *Inform Know Syst Manage* 2012;**11**:101-17.
13. Glazner C. Enterprise transformation using a simulation of enterprise architecture. *J Enterprise Transform* 2011;**1**:231-60.
14. McDermott T, Rouse W, Goodman S, et al. Multi-level modeling of complex socio-technical systems. *Proc Comput Sci* 2013;**16**:1132-41.
15. Park H, Clear T, Rouse WB, et al. Multi-level simulation of health delivery systems: a prospective tool for policy, strategy, planning, and management. *Service Sci* 2012;**4**:253-68.10.
16. Department of Defense. Defense Federal Acquisition Regulation Supplement: Detection and avoidance of counterfeit electronic parts (DFARS Case 2012-D055), Federal Register 2014;**79**:26091-108.
17. Livingston H. Avoiding counterfeit electronic components. *IEEE Trans Compon Packag Tech* 2007;**30**:187-89.
18. McFadden FE, Arnold RD. Supply chain risk mitigation for IT electronics. Proc IEEE Internat Conf Technol Homeland Secur 2010:49-55.
19. SAE International. Compliance verification criterion standard for SAE AS6081, fraudulent/counterfeit electronic parts: avoidance, detection, mitigation, and disposition – distributors. http://standards.sae.org/wip/as6301/. Retrieved 6/4/2014.
20. Cohen BS, Lee K. On the limits of test in establishing products assurance. Arlington, VA: Institute for Defense Analysis, 2014.
21. Pennock MJ, Rouse WB. The challenges of modeling enterprise systems. *Proc 4th Intl Engineer Syst Symp* 2014.
22. Pennock MJ, Rouse WB, Bodner DA, et al. Enterprise systems analysis. Technical Report SERC-2015-TR-020-4. Hoboken, NJ: Systems Engineering Research Center, Stevens Institute of Technology, 2015.
23. Snider J. Chip supplier pleads diminished capacity to avoid imprisonment after selling counterfeit parts to the U.S. Navy and others. ERAI Blog (http://www.erai.com/ERAI_Blog/3046/Chip%20Supplier%20Pleads%20Diminished%20Capacity%20to%20Avoid%20I). Accessed 5/28/2015; 2015.